对NAT网守默认配置导致的高利用率问题进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

症状

数据包跟踪功能

- 基本数据包跟踪配置

什么是NAT网守

检查NAT网守

解决方法/修复

- 解决方案 1
- 解决方案 2

摘要

相关信息

简介

本文档介绍如何识别和解决路由平台上由于NATed和非NATed流量混合而导致的高QFP使用率。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS® XE数据包转发架构的基本知识
- 数据包跟踪功能的基本体验

使用的组件

本文档不限于特定的软件和硬件版本。它适用于任何具有物理/虚拟化高量子流处理器(QFP)的路由Cisco IOS XE平台，如ASR1000、ISR4000、ISR1000、Cat8000或Cat8000v。

本文档基于处于自主模式的Cisco IOS XE设备，SDWAN（控制器）或SD路由可以遵循类似的逻辑，但具体内容可以不同。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

当同一接口上同时存在NATed和非NAT流量时，可以在Cisco路由器上观察到Cisco Quantum Flow Processor(QFP)的高利用率和性能问题。这也会导致其他性能问题，例如接口错误或速度缓慢。



注意：QFP位于嵌入式服务处理器(ESP)上，负责所有入站和出站流量的数据平面和数据包处理，这可根据平台进行物理或虚拟化。

症状

从路由器验证并确认这些症状对于识别此行为非常重要：

1. — 高QFP负载警报。当负载超过80%的阈值时，会显示这些警报。

```
Feb 8 08:02:25.147 mst: %IOSXE_QFP-2-LOAD_EXCEED: Slot: 0, QFP:0, Load 81% exceeds the setting threshol
Feb 8 08:04:15.149 mst: %IOSXE_QFP-2-LOAD_RECOVER: Slot: 0, QFP:0, Load 59% recovered.
```



注意：您还可以运行show platform hardware qfp active datapath utilization summary命令以显示QFP上的负载和流量速率。

```
Router# show platform hardware qfp active datapath utilization summary
  CPP 0: Subdev 0            5 secs        1 min        5 min       60 min
Input:  Priority (pps)            0            0            0            0
                 (bps)           96           32           32           32
    Non-Priority (pps)       327503       526605       552898       594269
                 (bps)   1225600520   2664222472   2867573720   2960588728
           Total (pps)       327503       526605       552898       594269
                 (bps)   1225600616   2664222504   2867573752   2960588760
```

```
Output: Priority (pps)            6            7            7            7
                 (bps)         8576         9992         9320         9344
    Non-Priority (pps)       327715       526839       553128       594506
                 (bps)   1257522072   2714335584   2920005904   3016943800
           Total (pps)       327721       526846       553135       594513
                 (bps)   1257530648   2714345576   2920015224   3016953144
Processing: Load (pct)           99           72           34           19
```

2. — 接口错误。如果QFP使用率较高，则数据包可能会由于背压而丢弃。在这种情况下，接口上通常会观察到超载和输入丢弃。要显示此信息，可以运行show interfaces命令。

```
Router# show interface gigabitEthernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4351-3x1GE, address is e41f.7b59.cba1 (bia e41f.7b59.cba1)
  Description: ### LAN Interface ###
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 2/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is force-up, media type is LX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:06:47, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 9390000 bits/sec, 2551 packets/sec
  30 second output rate 1402000 bits/sec, 1323 packets/sec
     368345166434 packets input, 199203081647360 bytes, 0 no buffer
     Received 159964 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     2884115457 input errors, 0 CRC, 0 frame, 2884115457 overrun, 0 ignored
     0 watchdog, 3691484 multicast, 0 pause input
     220286824008 packets output, 32398293188401 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     3682606 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     21 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

3. — 在某些情况下，用户可能会抱怨网络速度缓慢。

数据包跟踪功能

数据包跟踪工具可提供有关数据包如何由Cisco IOS XE平台处理的详细信息。它具有3个检测级别，即记帐、摘要和数据路径。检测级别基于debug platform condition状态。

您可以获得如下信息：

- 输入和输出接口
- 数据包状态
- 时间戳
- 数据包跟踪

> 注意：配置数据路径会消耗更多的数据包处理资源，这些资源仅反映在与过滤条件匹配的数据包上。

有关数据包跟踪的详细信息，请参阅使用Cisco IOS XE数据路径数据包跟踪功能进行故障排除。

基本数据包跟踪配置

这是具有数据路径级别检测的基本数据包跟踪配置的示例。它以循环方式收集8192个数据包（覆盖旧数据包），从第3层创建每个数据包的副本，该副本到达并离开接口GigabitEthernet 0/0/1。

```
Router# debug platform packet-trace packet 8192 circular fia-trace data-size 2048
Router# debug platform packet-trace copy packet both L3 size 64
Router# debug platform condition interface gigabitEthernet 0/0/1 both
Router# debug platform condition start
Router# debug platform condition stop
```

您可以使用这些命令检查数据包跟踪的结果。

```
Router# show platform packet-trace summary
Router# show platform packet-trace packet all
```

通过数据包跟踪捕获，您可以看到NAT功能消耗的资源比预期多。在下一个示例中，您可以看到IPV4_NAT_INPUT_FIA功能的失效时间明显大于其他功能的失效时间。此行为通常表示QFP需要更多时间处理此功能，因此，QFP中的更多资源用于NAT。

```
Packet: 161         CBUG ID: 161
Summary
  Input     : GigabitEthernet0/0/1
  Output    : GigabitEthernet0/0/2.1730
  State     : FWD
  Timestamp
    Start   : 25136781447706429 ns (02/10/2024 00:25:49.584050 UTC)
    Stop    : 25136781447993237 ns (02/10/2024 00:25:49.584337 UTC)
```

```
  Feature: IPV4_NAT_INPUT_FIA   <<<<<<<<<<<<
    Entry       : Input - 0x700162ac
    Input       : GigabitEthernet0/0/1
    Output      :



    Lapsed time : 1873376 ns     <<<<<<<<<<<<



  Feature: IPV4_INPUT_IPOPTIONS_PROCESS
    Entry       : Input - 0x70016344
    Input       : GigabitEthernet0/0/1
    Output      : GigabitEthernet0/0/2.1730
    Lapsed time : 64 ns
```

什么是NAT网守

在Cisco IOS XE路由平台中，默认启用网络地址转换(NAT)网守功能。NAT网守最初是为了防止非NAT处理的流使用过多的处理资源来创建NAT转换而创建的。NAT网守根据源地址为内部到外部方向和其他方向创建两个小缓存。每个缓存条目都包含一个源地址、一个虚拟路由和转发(VRF)ID、一个计时器值（用于使条目失效）和一个帧计数器。

NATed接口上的大量非NATed流量会消耗大量资源，并导致QFP使用率峰值。Cisco建议客户不要尽可能在同一接口上使用NAT-ed和非NAT-ed流。

检查NAT网守

可以使用show platform hardware qfp active feature nat datapath { gatein命令检查NAT网守统计信息 | gateout } 活动。这显示了缓存的大小、命中数、未命中数、已过期、已添加条目和活动条目数。通常，如果存在大量未命中数，并且此数目在短时间内迅速增加，则这表示大量未命名的流未添加到缓存。此行为导致这些流由NAT工作流程中的QFP处理，并且这会提高高QFP利用率。

```
Router# show platform hardware qfp active feature nat datapath gatein activity
Gatekeeper on
def mode Size 8192, Hits 191540578459, Miss 3196566091, Aged 1365537 Added 9 Active 7

Router# show platform hardware qfp active feature nat datapath gateout activity
Gatekeeper on
```

```
def mode Size 8192, Hits 448492109001, Miss 53295038401, Aged 149941327 Added 603614728 Active 1899
```

解决方法/修复

在大多数环境中，NAT网守功能运行正常，不会导致问题。但是，如果确实遇到此问题，有几种方法可以解决。

解决方案 1

对于此类问题，Cisco建议将NATed和非NATed流量从同一接口分离。它可用于不同的接口或网络设备。

解决方案 2

增加NAT网守功能上的缓存大小，以减少从网守丢失的数量。

下一个示例显示如何调整Cisco路由器上的网守。请注意，此值必须以2的幂来表示。否则，该值会自动设置为下一个更小的大小。

```
Router(config)# ip nat service gatekeeper
Router(config)# ip nat settings gatekeeper-size 65536
```



注意：调整缓存大小可能会消耗QFP中的内存，从而优化其使用。尝试逐渐调整此值，以与默认设置最接近的可能值开始。

执行上述解决方案之一后，建议监控这两个参数，以确认问题已解决：

1. — 检验QFP利用率是否已降低。

2. — 确认未命中数不会继续增加。

摘要

当NATed接口上存在非NATed流时，NAT网守功能可以提高路由器的性能。当NAT转换某些

NATed流时，同时非NATed流通过同一接口时，通常会发生这种情况。在大多数环境中，NAT Gatekeeper功能不会对路由器造成任何影响。但是，必要时仔细调整该特性以避免副作用，这很重要。

相关信息

- ASR1K NAT间歇性无法转换某些数据包
- 使用Cisco IOS XE数据路径数据包跟踪功能进行故障排除
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。